This workshop will deal with 3 different but tightly connected aspects of the emerging field of Privacy-aware Machine Learning (PAML) - meaning the application of ML techniques to data sets with artificially decreased information content. Such ‘perturbation’ can either be faced by disruptive outside forces, but more prominently by the user of a system exercising their ‘right to be forgotten’ or prophylactic anonymization on the part of an organization. We have already examined the effects of such perturbation of a standardized dataset on the performance of different classifiers and come to surprising results; the next interesting questions were 1) how do other ML techniques (multi-class classification, prediction, etc.) behave under perturbation, 2) is ML on graph structures more robust under the effects of perturbation, and 3) can interactive Machine Learning (iML) incorporating the Human-in-the-loop yield better heuristics for internal cost functions so that information loss in anonymization can be minimized as measured by algorithmic performance. We will examine all of those questions including our experimental setup for iML; students will be able to conduct a live iML experiment to test the influence of their own human judgment on ML behavior.

Bernd Malle is a full-time employee at Secure Business Austria (SBA) Research and currently pursuing his PhD in CS at Graz University of Technology.